IN THE CLAIMS

What is claimed is:

1. A method for sending a secure e-mail, comprising the steps of:

(a) composing an e-mail message by a sender, wherein said e-mail message includes a body field and at least one receiver field containing at least one receiver id representing at least one intended receiver;

(b) providing a sender id, a sender password, and all said receiver ids to a security server;

(c) receiving a message key and a message id which is unique for said e-mail message from said security server;

(d) encrypting said body field of said e-mail message based on said message key and enclosing said message id therewith to form the secure e-mail;

(e) mailing said secure e-mail in conventional manner to said receivers; and

(f) storing said message id, said message key, and all said receiver ids at said security server, to allow said security server to provide said message key to said receivers so that they may decrypt and read the secure e-mail.

2. The method of claim 1, wherein:

in said step (a) said e-mail message further includes a subject field; and

said step (d) includes encrypting said subject field.

3. The method of claim 1, wherein said sender id is associated with an e-mail address for said sender.

4. The method of claim 1, wherein said sender password is derived from a private password provided by said sender, to permit said sender to maintain said private password as private.

5. The method of claim 1, wherein said sender password has been previously stored for said sender.

6. The method of claim 1, further comprising authenticating said sender based on said sender id and said sender password after said step (b) and prior to proceeding with said step (c).

7. The method of claim 1, wherein said step (d) encrypts using a symmetric key encryption algorithm.

8. The method of claim 1, wherein:

said step (e) includes mailing to at least one said receiver which is a receiver list; and the method further comprising:

resolving said receiver list into a plurality of said receiver ids for said security server, to allow said security server to provide said message key to instances of said receivers which are members of said receiver list.

9. The method of claim 1, further comprising:

said step (b) includes providing a message hash based on said e-mail message to said security server; and

said step (c) includes receiving a first message seal from said security server based on said message hash; and

said step (d) includes enclosing the first message seal with the secure e-mail, to permit said security server comparing said first message seal with a second message seal taken from the secure e-mail as received to determine whether the secure e-mail has been altered while in transit to said receiver.

10. The method of claim 1, wherein at least one of said steps (b) and (c) employs secure socket layer protocol in communications with said security service.

11. A method for receiving a secure e-mail, comprising the steps of:

(a) accepting the secure e-mail by a receiver, wherein the secure e-mail includes a body field that is encrypted and a message id that uniquely identifies the secure e-mail;

(b) providing said message id as well as a receiver id and a receiver password for said receiver to a security server;

(c) receiving a message key from said security server; and

(d) decrypting the secure e-mail based on said message key, to form an e-mail message which is readable by said receiver.

12. The method of claim 11, wherein:

in said step (a) said secure e-mail further includes a subject field that is also encrypted; and

said step (d) includes decrypting said subject field.

13. The method of claim 11, wherein said receiver id is associated with an e-mail address for said receiver.

14. The method of claim 11, wherein said receiver password is derived from a private password provided by said receiver, to permit said receiver to maintain said private password as private.

15. The method of claim 11, wherein said receiver password has been previously stored for said receiver.

16. The method of claim 11, further comprising authenticating said receiver based on said receiver id and said receiver password after said step (b) and prior to proceeding with said step (c).

17. The method of claim 11, wherein said step (d) decrypts using a symmetric key decryption algorithm.

18. The method of claim 11, wherein:

the secure e-mail was sent by a sender and a first message seal based on the secure e-mail before it left control of said sender is stored by said security server;

said step (b) further includes also providing to said security server a second message seal which is taken from the secure e-mail as received by said receiver; and

said step (c) includes receiving an indication from said security server whether said first message seal and said second message seal match, to determine whether the secure e-mail was altered in transit.

19. The method of claim 11, wherein at least one of said steps (b) and (c) employs secure socket layer protocol in communications with said security service.

20. A system for communicating an e-mail message securely between a sender and a receiver, the system comprising:

a sending unit that composes the e-mail message for the sender, wherein the e-mail message includes a body field and a receiver field containing a receiver id representing the receiver;

said sending unit including a logic that provides a sender id, a sender password, and said receiver id to a security server;

said security server including a logic that replies to said sending unit with a message id, which is unique for the e-mail message, and a message key;

said security server further including a logic that stores said message id, said message key, and said receiver id;

said sending unit further including a logic that encrypts the e-mail message based on said message key and encloses said message id therewith to form a secure e-mail;

said sending unit yet further including a logic that e-mails said secure e-mail in conventional manner to the receiver;

a receiving unit that accepts said secure e-mail;

said receiving unit including a logic that provides said message id, said receiver id and a receiver password to said security server;

said security server yet further including a logic that replies to said receiving unit with said message key for said secure e-mail;

said security server still further including a logic that decrypts said secure e-mail based on said message key into the e-mail message such that it is readable by the receiver.